Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 505–516
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Treillis de codes quasi-cycliques

Anne Desideri Bracco

I3S, ESSI, BP 145, Route des Colles, 06 903 Sophia Antipolis, France

Reçu le 18 juin 2003; reçu en forme révisée le 1 août 2003; accepté le 15 août 2003

Résumé

Nous présentons une construction graphique de codes quasi-cycliques. Cette construction par treillis généralise la construction cubique de Forney et elle correspond à un cas particulier de l'approche algébrique proposée par Ling et Solé. Des codes binaires auto-duaux et extrêmaux de paramètres [24, 12, 8], [40, 20, 8] et [72, 36, 12] sont contruits en exemple.

1. Introduction

Dans [1], Forney étudie la construction cubique d'un point de vue graphique, sous l'angle des treillis. Dans [2], Ling et Solé montrent que la construction cubique est associée aux codes quasi-cycliques et proposent une approche algébrique et générale de ces codes.

Dans cet article, nous étudions d'un point de vue graphique un cas particulier de cette construction algébrique et généralisons le treillis de Forney pour la cubique.

Dans la première section, nous rappelons les définitions de code quasi-cyclique et de treillis associé. Ensuite nous présentons la construction graphique, dénotée "m-ique", basée sur des partitions. Nous l'illustrons par plusieurs exemples dans la dernière partie: la construction cubique sous–jacente de l'hexacode puis l'élaboration de codes auto-duaux de paramètres [24, 12, 8], [72, 36, 12] et [40, 20, 8] définis sur $\mathbb{F}_2$.

2. Définitions

$\mathbb{F}$ désigne un corps fini de caractéristique p et, lorsqu'il est nécessaire de le préciser, $\mathbb{F}_q$ est un corps fini d'ordre q.

E-mail address: adbracco@essi.fr (A. Desideri Bracco).

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.08.004

Définition 2.1. Un code en blocs, linéaire, de longueur n et défini sur $\mathbb{F}$ est un $\mathbb{F}$-sous-espace vectoriel de $\mathbb{F}^n$. Ses éléments sont appelés mots.

Dans la suite, tous les codes considérés sont définis sur $\mathbb{F}$ et $\mathbb{F}$-linéaires.

Définition 2.2. Le poids d'un mot est le nombre de ses composantes non nulles et la distance minimale d'un code correspond au poids minimum de ses mots.

Un code est de paramètres $[n, k, d]$ lorsqu'il est de longueur n, de dimension k et de distance minimale d.

Le dual d'un code est défini par rapport au produit scalaire usuel ou par rapport au produit hermitien $\sum x_i y_i^{-1}$ [2, p. 2752]. Un code est dit auto-dual lorsqu'il est égal à son dual.

Définition 2.3. Soit D l'opérateur décalage. Un code est cyclique lorsqu'il est invariant par D et quasi-cyclique d'index ℓ(ou ℓ-$Q.C$) lorsqu'il est invariant par D^ℓ.

Exemple 1. Sur $\mathbb{F}_2$, $C_1 = \{000, 011, 110, 101\}$ est cyclique et $C_2' = \{0000, 0011, 1100, 1111\}$ est 2-$Q.C$.

Définition 2.4. Un graphe orienté étiqueté $(\mathcal{S}, \mathcal{A}, \mathcal{E})$ consiste en un ensemble $\mathcal{S}$ de sommets, un ensemble $\mathcal{E}$ d'étiquettes et un ensemble $\mathcal{A}$ de triplets ordonnés (s, s', e), où $s, s' \in \mathcal{S}$ et $e \subset \mathcal{E}$. Un chemin du sommet s au sommet s' est défini comme une suite $(a_i)_{i=0\ldots m} = (s_i, s_{i+1}, e_i)_{i=0\ldots m}$ d'éléments de $\mathcal{A}$ où a_0 débute en $s_0 = s$, et a_m se termine en $s_{m+1} = s'$.

Un treillis $\mathcal{T}$ de profondeur n est un graphe orienté étiqueté tel que l'ensemble de ses sommets $\mathcal{S}$ admette une partition $(\mathcal{S}_i)_{i=0\ldots n}$ et où chaque arc commençant en un sommet de $\mathcal{S}_i$ se termine en un sommet de $\mathcal{S}_{i+1}$.

Les ensembles $\mathcal{S}_i$ sont les niveaux, et par convention, $\mathcal{S}_0$ et $\mathcal{S}_n$ sont réduits à un seul élément.

À chaque chemin $(s_i, s_{i+1}, e_i)_{i=0\ldots n}$ entre $\mathcal{S}_0$ et $\mathcal{S}_n$ est associée la suite concaténée des étiquettes $e_0 e_1 \ldots e_n$.

$\mathcal{T}$ engendre le code $\mathcal{C}$ lorsque l'ensemble des suites ainsi définies par les chemin entre $\mathcal{S}_0$ et $\mathcal{S}_n$ correspond à l'ensemble des mots de $\mathcal{C}$.

Exemple 2. Le treillis de la Fig. 1 correspond au code défini sur $\mathbb{F}_2$, de longueur 4, et dont les mots sont {0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111}.

Les arcs parallèles (sommets de départ et d'arrivée identiques) seront symbolisés par un seul arc, étiqueté par l'ensemble des labels des arcs ainsi substitués. La Fig. 2 reprend la représentation précédente ainsi schématisée. Réciproquement, un arc étiqueté par un ensemble correspondra à un groupement d'arcs parallèles.

Différentes méthodes permettent d'obtenir le treillis d'un code donné. Elles sont rappelées dans [3]. Notre but est de partir du graphe et d'étudier le code associé.

3. Construction *m*-ique

Cette construction permet d'obtenir un code $\mathcal{C}$ ℓ-$Q.C$ et de longueur ℓm à partir d'un code C de longueur ℓ. Elle repose sur la représentation graphique de partitions de C.

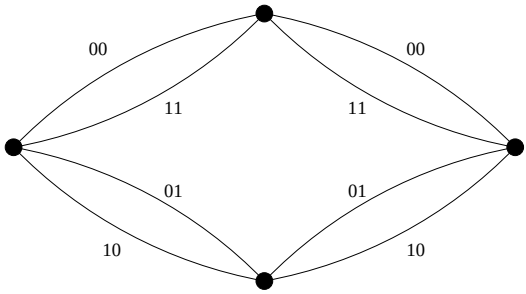

Fig. 1. Construction carrée de Forney—Représentation détaillée.

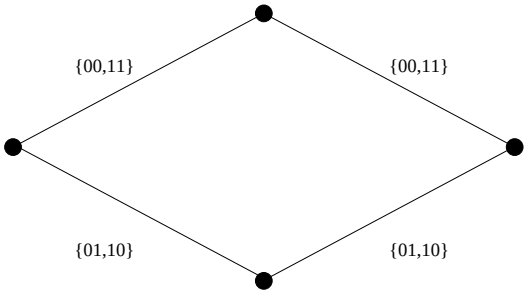

Fig. 2. Construction carrée de Forney.

Nous exposons tout d'abord les partitions utilisées et la construction du treillis, puis nous montrons que ce graphe correspond à un code ℓ-Q.C de longueur ℓm.
Des exemples de constructions sont donnés dans le paragraphe suivant.

3.1. Partitions de C

C est un code de longueur ℓ défini sur $\mathbb{F}$, C' un sous-code de C et C'' un sous-code de C'. C/C' est la partition de C induite par C' suivant la relation d'équivalence: $x\Re y \Leftrightarrow x - y \in C'$. De même, C'' induit les partitions C'/C'' de C' et C/C'' de C.
Nous notons $[C/C']$ et $[C'/C'']$ les ensembles des représentants de ces partitions;

$$\text{ainsi } C/C' = \{C'_\alpha, \alpha \in [C/C']\}, \qquad C'/C'' = \{C''_\beta, \beta \in [C'/C'']\},$$
$$C = \cup_{\alpha\in[C/C']} C'_\alpha, \qquad \text{avec } C'_0 = C',$$
$$\text{et} \quad C' = \cup_{\beta\in[C'/C'']} C''_\beta, \qquad \text{avec } C''_0 = C''.$$

$[C'] = \mathbf{0}$, où $\mathbf{0}$ est le mot tout à 0, $[C''] = \mathbf{0}$, $C'_\alpha = \alpha + C'$, $C''_\beta = \beta + C''$,

$$\text{et} \qquad C'_0 = \cup_{\beta\in[C'/C'']} C''_\beta,$$
$$C'_\alpha = \cup_{\beta\in[C'/C'']}([C'_\alpha] + C''_\beta),$$
$$\text{ou encore } C'_\alpha = \cup_{\beta\in[C'/C'']}([C'_\alpha] + [C''_\beta] + C''),$$
$$\text{soit} \qquad C = \cup_{\alpha\in[C/C']}(\cup_{\beta\in[C'/C'']}([C'_\alpha] + [C''_\beta] + C'')).$$

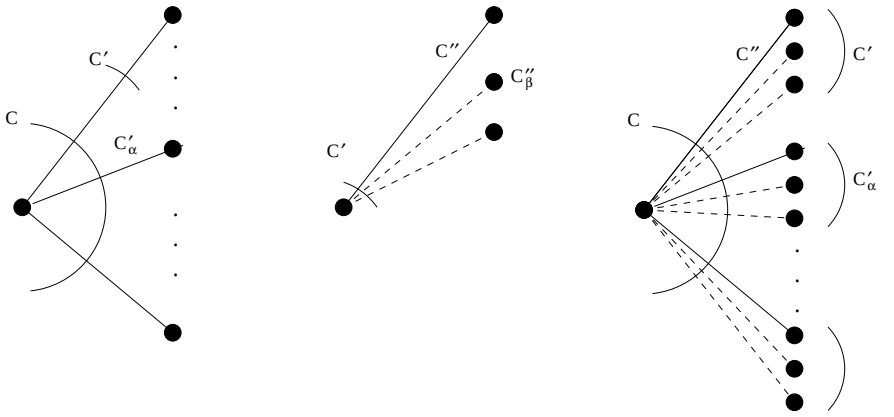

Fig. 3. Partitions C/C', C'/C'' et C/C''.

Remarque 1. $[C/C']$ est un code et C est le code engendré par les codes $[C/C']$ et C': $C = [C/C'] + C' = \langle [C/C'], C' \rangle$. De même, $C' = \langle [C'/C''], C'' \rangle$.

Ces partitions sont représentées graphiquement (Fig. 3):

- pour C/C', un premier sommet, noté ϕ, représente $[C/C] = \mathbf{0}$; de ϕ partent les arcs correspondant aux classes d'équivalence de C', vers les sommets étiquetés par les représentants $[C'_i]$,
- pour C/C'', le même principe de construction est appliqué à chaque classe d'équivalence C'_i.

3.2. Treillis $\mathcal{T}_m$

Ce treillis est basé sur les partitions de C.

3.2.1. Sommets de $\mathcal{T}_m$

ϕ est le seul sommet de niveau 0 du treillis.
Le niveau 1 et les $m - 2$ niveaux suivants possèdent $|[C/C'][C'/C'']|$ sommets. Ils correspondent aux représentants de la partition C/C''.
Le dernier niveau, le niveau m, possède un seul sommet, noté Φ, qui correspond à $\mathcal{C}/\mathcal{C}$.
La grappe ($\ll$ *cluster* $\gg$) α correspond aux sommets de la partition de C'_α par $\alpha + C''_0$, c'est-à-dire aux $\alpha + \beta$, $\beta \in [C'/C'']$; ainsi les sommets de la grappe 0 correspondent aux β, $\beta \in [C'/\mathcal{C}'']$.
Les sommets sont partagés horizontalement en grappes, à l'exclusion de ϕ et Φ, et verticalement en niveaux (Fig. 4).

3.2.2. Arcs et étiquettes de $\mathcal{T}_m$

ϕ est relié à tous les sommets du niveau 1. À l'intérieur de la grappe α, chacun des sommets de niveau t est relié à chacun des sommets du niveau successif $t + 1$, comme représenté Fig. 5.

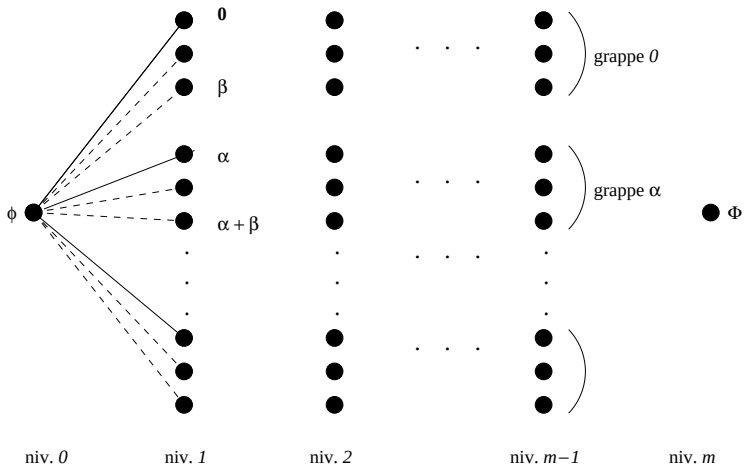

Fig. 4. Les sommets de $\mathcal{T}_m$.

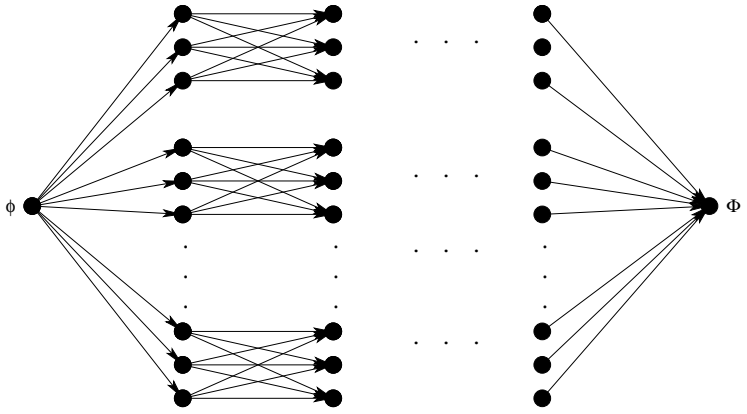

Fig. 5. Les arcs de $\mathcal{T}_m$.

Chaque arc possède comme étiquette une classe d'équivalence qui correspond à:

C''_β entre ϕ et	β,
$\alpha + C''_\beta$ entre ϕ et	$\alpha + \beta$,
$\alpha + C''_{\beta'-\beta}$ entre $\alpha + \beta$ et	$\alpha + \beta'$, à l'intérieur d' une même grappe,
$-(\alpha + \beta) + C''$ entre $\alpha + \beta$ et	Φ.

3.2.3. Complexité de $\mathcal{T}_m$

Soient $|\alpha|$ le cardinal de $[C/C']$ et $|\beta|$ le cardinal de $[C'/C'']$.

Le treillis $\mathcal{T}_m$ possède $1 + |\alpha|\,|\beta|(m-1) + 1$ soit $2 + (m-1)|\alpha|\,|\beta|$ sommets et $|\alpha|\,|\beta| + (m-2)|\beta|^2 + |\alpha|\,|\beta|$ soit $|\alpha|\,|\beta|(2 + (m-2)|\beta|)$ arcs.

3.3. Le code $\mathcal{C}$

Soit $\mathcal{C}$ le code engendré par le treillis $\mathcal{T}_m$. Ses mots correspondent aux concaténations des étiquettes des divers chemins entre ϕ et Φ.

Théorème 3.1. *$\mathcal{C}$ vérifie:*

1. $\mathcal{C} = \{(x + a_1|x + a_2|\cdots|x + a_{m-2}|x + a_{m-1}|x + a_m),\ x \in [C/C'],\ a_i \in C'$ *pour* $i = 1 \ldots m$ *et* $\sum_{i=1}^{m} a_i \in C''\}$,
2. $\mathcal{C}$ *est un code linéaire ℓ-quasi-cyclique de longueur ℓm,*
3. *la distance minimale $d_{\mathcal{C}}$ vérifie $d_{\mathcal{C}} \geq \min\{d_{C''}, 2d_{C'}, md_C\}$, où d_C (resp. $d_{C'}$, $d_{C''}$) est la distance minimale dans C (resp. C', C''),*
4. $\mathcal{C}$ *possède $|C/C'| \cdot |C'/C''|^{m-1} \cdot |C''|^m$ mots.*

1. Considérons un chemin reliant ϕ à Φ dans la grappe 0; notons $S_{1,\alpha_1}, S_{2,\alpha_2}, \ldots, S_{m-1,\alpha_{m-1}}$ les sommets traversés. L'ensemble des mots engendrés par ce chemin est $C''_{\alpha_1} \cdot C''_{\alpha_2-\alpha_1} \cdots C''_{\alpha_{m-1}-\alpha_{m-2}} \cdot C''_{-\alpha_{m-1}}$. Cet ensemble s'exprime par:

$$\{(\alpha_1 + \epsilon_1|\alpha_2 - \alpha_1 + \epsilon_2|\cdots|\alpha_{m-1} - \alpha_{m-2} + \epsilon_{m-1}| - \alpha_{m-1} + \epsilon_m),\ \epsilon_i \in C''\}.$$

   En considérant tous les chemins possibles entre ϕ et Φ de cette grappe, il vient:

$$\{(\alpha_1 + \epsilon_1|\alpha_2 - \alpha_1 + \epsilon_2|\cdots|\alpha_{m-1} - \alpha_{m-2} + \epsilon_{m-1}| - \alpha_{m-1} + \epsilon_m),\ \alpha_i \in [C'/C''],\ \epsilon_i \in C''\}.$$

   En posant $a_1 = \alpha_1 + \epsilon_1, a_2 = \alpha_2 - \alpha_1 + \epsilon_2, \ldots, a_m = -\alpha_{m-1} + \epsilon_m$, on obtient l'ensemble

$$\left\{(a_1|a_2|\cdots|a_{m-2}|a_{m-1}|a_m),\ a_i \in C' \text{ et } \sum_{i=0}^{m} a_i \in C''\right\}$$

   pour les mots engendrés par la grappe 0.
   Comme la grappe x correspond à la grappe 0 à laquelle x est ajouté à chaque étiquette, les mots engendrés par cette grappe sont

$$\left\{(x + a_1|x + a_2|\cdots|x + a_{m-2}|x + a_{m-1}|x + a_m),\ a_i \in C' \text{ et } \sum_{i=0}^{m} a_i \in C''\right\}.$$

   L'ensemble recherché s'obtient en considérant toutes les valeurs possibles pour x.
2. La linéarité de $\mathcal{C}$ découle de la linéarité de C.
   $\mathcal{C}$ est de longueur ℓm puisque ses mots sont la concaténation de m mots de longueur ℓ.
   $\mathcal{C}$ est ℓ-quasi-cyclique car, si $(x + a_1|x + a_2|\cdots|x + a_{m-2}|x + a_{m-1}|x + a_m)$ est un mot de $\mathcal{C}$, alors $(x + a_2|\cdots|x + a_{m-2}|x + a_{m-1}|x + a_m|x + a_1)$ est également un mot de $\mathcal{C}$: il suffit de poser $a'_i := a_{i+1}$ pour $i = 1, \ldots, m-2$ et $a'_m := a_1$. Alors $\sum_{i=0}^{m} a'_i = \sum_{i=0}^{m} a_i \in C''$ et ainsi $(x + a_2|\cdots|x + a_{m-2}|x + a_{m-1}|x + a_m|x + a_1) = (x + a'_1|x + a'_2|\cdots|x + a'_{m-2}|x + a'_{m-1}|x + a'_m) \in \mathcal{C}$.

3. Considérons deux mots distincts; soit ils sont engendrés par le même chemin et diffèrent alors d'au moins $d_{C''}$, soit leurs chemins sont différents; s'ils appartiennent à la même grappe, les mots sont alors distants d'au moins $2d_{C'}$; sinon, leurs mots diffèrent de md_C.
4. Chaque chemin de ϕ à Φ engendre $|C''|^m$ mots; chacune des $|C/C'|$ grappes possède—$|C'/C''|^{m-1}$ chemins différents. Il y a donc $|C/C'| \cdot |C'/C''|^{m-1} \cdot |C''|^m$ mots.

Cette construction coïncide avec la construction algébrique de [2] dans certains cas. Nous la rappelons dans le cas où m est un nombre premier et où l'ordre de $\mathbb{F}$, q, est primitif modulo m.

Théorème 3.2 ([2], Th. 5.1). *Supposons m premier et* $\mathbb{F} = \mathbb{F}_q$, avec q *primitif modulo* m. $Y^m - 1$ *admet alors une décomposition en exactement deux facteurs premiers irréductibles sur* $\mathbb{F}_q$*:*

$$Y^m - 1 = (Y - 1)(Y^{m-1} + \cdots + Y + 1)$$

et pour tout ℓ*, les codes* ℓ*-quasi-cycliques de longueur* ℓm *sont déterminés par la construction suivante:*

soit C_1 *un code défini sur* $\mathbb{F}_q$ *de longueur* ℓ *et* C_2*, un code défini sur* $\mathbb{F}_{q^{m-1}}$*, également de longueur* ℓ*. Pour chaque* $x \in C_1$, $y \in C_2$ *et pour chaque* $0 \leq g \leq m - 1$*, posons*

$$c_g(x, y) = x + (\mathrm{Tr}_{\mathbb{F}_{q^{m-1}}/\mathbb{F}_q}(y\zeta^{-g}))$$

où

$$\mathrm{Tr}_{\mathbb{F}_{q^{m-1}}/\mathbb{F}_q}(x) := x + x^q + x^{q^2} + \cdots + x^{q^{m-2}}$$

désigne l'opérateur trace défini pour $x \in \mathbb{F}_{q^{m-1}}$ *et à valeur dans* $\mathbb{F}_q$ *et où* ζ *est une racine primitive m-ième de l'unité.*

Le code C défini par

$$C = \{(c_0(x, y), \ldots, c_{m-1}(x, y)) \mid \forall x \in C_1, \forall y \in C_2\}$$

est un code ℓ*-quasi-cyclique de longueur* ℓm *défini sur* $\mathbb{F}_q$ *et, réciproquement, tout code* ℓ*-quasi-cyclique de longueur* ℓm *défini sur* $\mathbb{F}_q$ *est obtenu à partir de cette construction.*

De plus, C est auto-dual pour le produit scalaire usuel si et seulement si C_1 et C_2 sont autoduaux pour le produit scalaire hermitien $\sum x_i y_i^{-1}$ sur leurs corps respectifs.

Proposition 3.3. *La construction m-ique et la construction algébrique de [2] coïncident lorsque* C_2 *admet une matrice génératrice définie sur* $\mathbb{F}_q$*.*
Les relations entre les différents codes sont alors:

$$\begin{aligned} C &= C_1 + C_2' = \langle C_1, C_2' \rangle, \text{ où } C_2' \text{ désigne le sous} - \text{code de } C_2 \text{ défini sur } \mathbb{F}_q \\ C' &= C_2' \\ C'' &= C_1 \cap C_2'. \end{aligned}$$

Lorsque $m = 2$ et p impair, nous retrouvons la construction $(u + v \mid u - v)$.

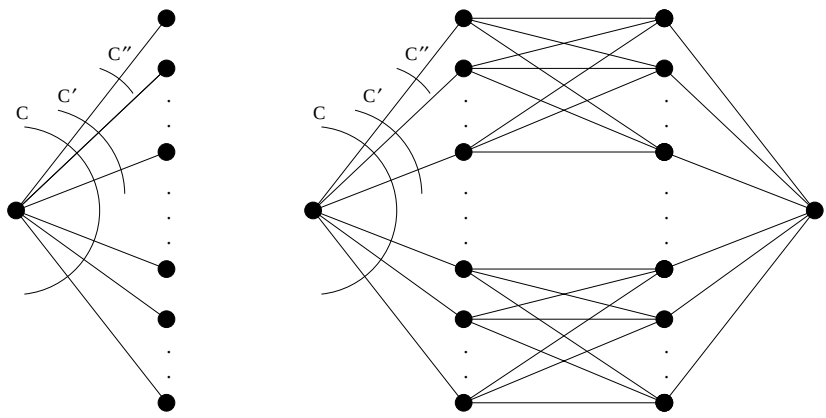

Fig. 6. Treillis cubique.

Lorsque $m = 3$ et $q \equiv 2 \bmod 3$, la construction algébrique donne l'expression $\mathcal{C} = \{(x + 2a - b|x - a + 2b|x - a - b), x \in C_1, a + \zeta b \in C_2\}$, où ζ est une racine primitive m-ième de l'unité. Suite à la restriction sur C_2, cela se simplifie en $\mathcal{C} = \{(x + 2a - b|x - a + 2b|x - a - b), x \in C_1, a, b \in C_2'\}$.
Lorsque $m = 3$ et $p = 2$, nous obtenons la construction de Turyn $(x + a|x + b|x + a + b)$.

4. Exemples de constructions

4.1. Construction cubique

La construction cubique, présentée par Forney dans [1], correspond au cas où $m = 3$. Le treillis a alors cette forme (Fig. 6):

Nous présentons trois exemples pour cette construction:

- l'hexacode: ce code est 2-$Q.C$; nous précisons la construction cubique sous-jacente.
- le code de Golay.
- un code de paramètres [72, 36, 12], non isomorphe à l'extension du code Résidu Quadratique sur $\mathbb{F}_2$ de longueur 71.

4.1.1. L'hexacode

L'hexacode $\mathcal{H}_6$ est un code de longueur 6 et de dimension 3 sur $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$, où $\bar{\omega} = 1 + \omega$, engendré par la matrice

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 1 & 0 & 1 & 0 & \bar{\omega} & \omega \end{pmatrix} \text{ équivalente à } \begin{pmatrix} 1 & 0 & 0 & 1 & \bar{\omega} & \omega \\ 0 & 1 & \bar{\omega} & \omega & 1 & 0 \\ \bar{\omega} & \omega & 1 & 0 & 0 & 1 \end{pmatrix}$$

qui traduit son caractère 2-$Q.C$.

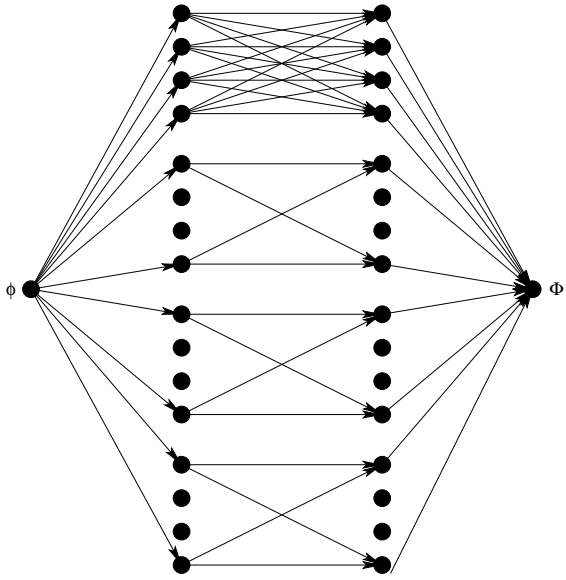

Fig. 7. Le treillis de l'hexacode, partiellement schématisé.

Il peut être obtenu par la construction cubique avec les codes intermédiaires suivants: $C := \mathbb{F}_4^2$, $C' := \{00, 11, \omega\omega, \bar{\omega}\bar{\omega}\}$ et $C'' := \{00\}$ sur $\mathbb{F}_4$
et alors $C_1 := \langle[1, 1]\rangle$ et $C_2' := \langle[1, 0]\rangle$ sur $\mathbb{F}_4$

Le treillis associé est composé de quatre grappes de quatre branches (Fig. 7).

Les 16 mots engendrés par la grappe 0 de l'hexacode sont:
$\{000000,\ 001111,\ 110011,\ 111100,\ 00\omega\omega\omega\omega, \ldots,\ 00\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}, \ldots,\ 11\omega\omega\bar{\omega}\bar{\omega}, \ldots,$
$11\bar{\omega}\bar{\omega}\omega\omega, \ldots\}$ (Fig. 8).

Définition 4.1 ([4]). Chaque mot $abcdef$ de $\mathcal{H}_6$ a une pente ($\ll slope \gg$) s et $abcdef$ est un mot de $\mathcal{H}_6$ de pente s si et seulement s'il vérifie les trois relations suivantes:

La 1-règle: $a + b = c + d = e + f = s$
La ω-règle: $a + c + e = a + d + f = b + c + f = b + d + e = \omega s$
La $\bar{\omega}$-règle: $b + d + f = b + c + e = a + d + e = a + c + f = \bar{\omega} s$.

Proposition 4.2. *La construction cubique regroupe les mots de $\mathcal{H}_6$ selon leurs pentes.*

Chaque grappe du graphe de la construction cubique de l'hexacode correspond à l'une des quatre valeurs possibles pour s : 0 pour la grappe associée à C', 1 pour la grappe associée à $01 + C'$, ω pour $0\omega + C'$ et $\bar{\omega}$ pour $0\bar{\omega} + C'$.

4.1.2. Le code de Golay

Sur $\mathbb{F}_2$, ce code de paramètres [24, 12, 8] est obtenu à partir de la construction cubique en prenant

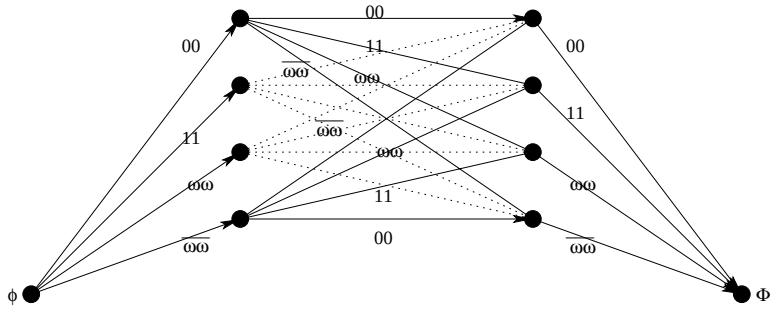

Fig. 8. Grappe 0 de l'hexacode.

$C = \mathcal{E}_8$, code des mots de poids pair de longueur 8 et de matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$C'' = \mathcal{H}_8$, code de Hamming [8, 4, 4] et de matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

et $C'' = \{00000000, 11111111\}(C'' = C^{\perp})$.
Alors $C_1 := \mathcal{H}_8^*$ et $C_2' := \mathcal{H}_8$, où la matrice génératrice de $\mathcal{H}_8^*$ est

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$\mathcal{H}_8^*$ est équivalent à $\mathcal{H}_8$.

Définition 4.3. Un code défini sur $\mathbb{F}_2$ est de type II lorsqu'il est auto-dual et que les poids de ses mots sont multiples de 4.

Exemple 3. Le code de Hamming $\mathcal{H}_8$ est un code de type II.

Proposition 4.4 ([2], Prop. 7.1). *Sur $\mathbb{F}_2$, si $\mathcal{C}$ est un code auto-dual et ℓ-quasi-cyclique de longueur 3ℓ, alors il est de type II si et seulement si son composant C_1 est de type II.*

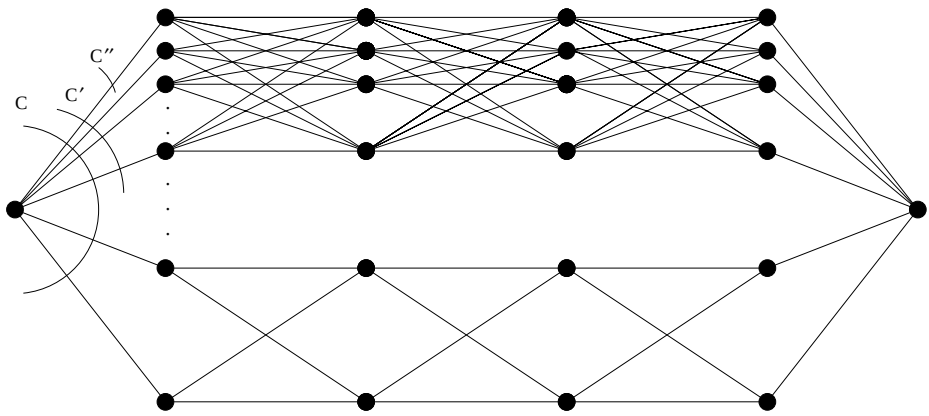

Fig. 9. Treillis quintique.

C_1 est un code de type II et l'extension de C_2' sur $\mathbb{F}_{2^2}$ est auto-duale; par la Proposition 4.4, le code obtenu est de type II. La distance minimale de ce code est multiple de 4 et, par le Théorème 3.1, supérieure à 6. Elle vaut au moins 8, qu'elle atteint par la borne de Hamming. Ainsi, le code obtenu est le code de Golay [6].

4.1.3. [72, 36, 12]

Ce code, défini sur $\mathbb{F}_2$ et auto-dual de paramètres [72, 36, 12], est obtenu à partir de la construction cubique en prenant
$C := \mathcal{E}_{24}$, code des mots de poids pair de longueur 24,
$C' := \mathcal{G}$, le code de Golay,
et $C'' := \{0 \ldots 0, 1 \ldots 1\}$, restreint aux mots tout à 0 et tout à 1 de longueur 24. (nouveau $C'' = C^{\perp}$)

$$C_1 := \mathcal{G}^* = \pi(\mathcal{G})$$

où π est la permutation (5, 17, 20, 22, 24, 15, 21, 12) (6, 18, 9, 11, 13, 23, 7, 8, 10).
Pour des raisons similaires au code précédent, ce code est de type II. Sa distance minimale est calculée par magma. Les calculs sur magma montrent également qu'il n'est pas isomorphe à l'extension du code Résidu Quadratique sur $\mathbb{F}_2$ de longueur 71.

4.2. Construction quintique

La construction quintique correspond à $m = 5$. Le treillis quintique a la forme représentée Fig. 9 suivante:

Un code binaire de paramètres [40, 20, 8], de type II et extrêmal, est obtenu à partir de la construction quintique et des codes utilisés ci-dessus pour le code de Golay:
$C = \mathcal{E}_8$, code des mots de poids pair de longueur 8
$C' = \mathcal{H}_8$, code de Hamming [8, 4, 4]
et $C'' = \{00000000, 11111111\}$.

La matrice génératrice de ce code, obtenue à l'aide de magma, est:

$$\begin{pmatrix}
1&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&1&1&1&0&1\\
0&1&0&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&1&1&1&1&0&1&1\\
0&0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&1&1&0&1&1&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&1&1&0&0&1&0&1\\
0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&1&0&1&0&0&0&1&1&1\\
0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&1&0&1&1&1&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0&1&1&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

5. Perspectives

Dans les derniers exemples cités, le code C'' est choisi de façon à optimiser la distance entre les mots de chaque étiquette. Nous espérons que cette condition, alliée à la forme du treillis qui suggère un traitement parallèle, permettra de simplifier le décodage.

Les traductions graphiques des autres formes algébriques proposées par [2] et le décodage, induit par ces treillis, restent à étudier.

Remerciements

Tous les programmes en magma [5] ont été effectués grâce à l'UMS Medicis (CNRS/Polytechnique), que l'auteur tient à remercier.

Références

[1] G.D. Forney Jr., Coset codes–part II: binary lattices and related codes, IEEE Transactions on Information Theory 34 (1988) 1152–1187.
[2] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Transactions on Information Theory 47 (2001) 2751–2760.
[3] A. Vardy, Trellis structure of codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, North-Holland, 1998 (Chapter 24).
[4] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, second ed., Springer, 1993.
[5] Available from http://magma.maths.usyd.edu.au/magma/.
[6] V. Pless, Introduction to the Theory of Error-Correcting Codes, third ed., Wiley, New York, 1998.